FEDERAL GOVERNMENT
FIREWALL PROTECTION PROFILES
FREQUENTLY ASKED QUESTIONS
12/19/97

1. What is the purpose of the specifications?

The firewall protection profile is a security requirements specification being prepared by the Federal Government that defines the basic needs of organizations handling unclassified information. The profile was written to comply with version 1.0 of the Common Criteria for Information Technology Security Evaluation (a.k.a. Common Criteria), a standard being developed jointly by the National Institute of Standards and Technology, the National Security Agency, and Government agencies from five other nations. As a minimal requirements specification, it fulfills multiple purposes: to serve as an example protection profile that demonstrates the suitability of the Common Criteria for non-operating systems products, to become the basis for firewall product evaluations by independent laboratories accredited to perform Common Criteria security evaluations, to be used in Government procurement activities, and to provide a suitable requirements baseline for use by industry.

2. Why are there two distinct firewall profiles: a traffic filter firewall and an application level firewall?

Originally there was a single profile covering a very broad class of products, ranging from simple packet filters to application proxy gateways. In order to adequately address that product range, the profile contained many conditional requirements, which made it difficult for readers to interpret and fully comprehend. During public review of the profile, the benefits of having two profiles, in spite of their strong similarities, became apparent, and action was taken to partition the specification accordingly. The traffic filter firewall profile applies to devices that are capable of screening traffic at the network and transport protocol levels, and auditing related events. The application level firewall profile applies to devices that are capable of screening traffic at the application protocol level, in addition to the network and transport levels, and authenticating end-users. The application level profile also contains some additional auditing requirements beyond those of the traffic filter. Both profiles require the same level of assurance.

3. What is the rational for the unique structure of the requirements contained in the specifications and the use of new, unfamiliar terminology?

The structure and content of a protection profile are dictated to a large degree by the Common Criteria. A protection profile contains predefined functionality and assurance components drawn from the Common Criteria to meet stated security objectives and policy required for a class of product or system. The functionality and assurance components are requirements written in natural language (i.e., English), but done so in a

manner that maintains uniformity in style and structure, and consistency in the use of security related terms. Unfortunately, the resulting text sometimes appears a bit awkward or unclear. However, this shortcoming is offset by the benefits of component reuse in other profiles, consistent interpretation by security evaluators, and the possibility for mutual recognition of evaluation results with other nations. For more information on the Common Criteria, see either http://csrc.nist.gov/nistpubs/cc/ or http://www.radium.ncsc.mil/tpep/library/ccitse/index.html.

4. How do some of the Common Criteria terms used in the specifications map to more common, information technology terms?

The Common Criteria uses many specialized terms that may not make sense upon first reading. Some of the more onerous terms used in the firewall protection profiles are translated below.

- **Target of Evaluation (TOE)** - a firewall implementation under assessment against the requirements specified in the protection profile (e.g., brand X firewall product).
- **TOE Security Policy (TSP)** - the security rules that define the behavior of a firewall implementation.
- **TOE Security Functions (TSF)** - the security mechanisms of a firewall that enforce its security policy (i.e., the TSP); formerly known as the trusted computing base under the Orange Book.
- **Security Function (SF)** - a portion of a firewall implementation that enforces a subset of the security policy, such as access control, audit, or identification and authentication.
- **Security Function Policy (SFP)** - the security rules enforced by a security function.

5. Why don't the specifications contain requirements for virtual private networking, secure dial-in remote access, etc.?

The firewall protection profiles identify minimal essential requirements for a class of firewall products that must always be met. They do not include additional security features, such as those mentioned, which are needed only by some organizations or appear only in some products. The profile specifications do not in any way, however, prohibit a developer from providing greater functionality or assurance in a product and having them assessed during an evaluation. This approach allows developers to address market demand, and organizations needing special features to distinguish among evaluated firewall products that meet a set of core requirements. Eventually, as differentiating product features become more widely implemented and used, they may be incorporated into an update of the profile.

6. Do the firewall profiles constrain the architecture of a firewall product or system in any way?

The sole architectural constraint asserted by the profiles is the capability to configure a firewall product or system in a dual-homed configuration. A developer is free to employ a centralized or distributed architecture, support multi-homed configurations, or provide other capabilities for inter-operation beyond those identified in the profiles. Whatever the choices made, however, the developer must render a complete, comprehensive firewall solution, and subject all security relevant components to evaluation.

7. Why are the filtering requirements stated in general terms rather than in detailed protocol-specific terms?

The aim of the specification is to define the generic security requirements of a firewall. While most present-day firewalls are primarily or exclusively oriented toward Internet protocols, the protocol filtering requirements in the profile apply equally to firewalls supporting proprietary or non-Internet protocols. Moreover, due to the vast number and ever changing set of protocols in use and under development today, a conscious decision was made to exclude detailed filtering requirements that pertain to protocol specific information contained within headers. During evaluation, protocol specific filtering capabilities claimed by the firewall's manufacturer are assessed against known vulnerabilities.

8. What is the relationship between the firewall profiles and organizational security policies?

The firewall profiles identify a set of capabilities needed for safe practice in a low risk environment. On the one hand, all of the capabilities identified may not be needed by an organization for a particular operating environment. On the other, the capabilities may be inadequate for a given environment. Ultimately, it is the organizational security policy that determines whether the profiles and products evaluated under profiles are appropriate for their environment, and if applicable, how or whether specific capabilities are used.

9. Any guidance on how best to read and interpret the protection profiles?

A protection profile should present the reader with a tightly woven view of identified threats, security objectives to counter those threats, functionality that fulfills the security objectives, and assurances needed from an evaluation. Unfortunately, this perspective is not readily apparent, but formulating it from parts of the specification should help improve understanding. In the firewall protection profile, the security objectives identified in section 4 are countermeasures to the threats listed earlier in section 3.2. The exact mapping between objectives and threats is given in section 6.1 and 6.2. Similarly, Table 5.1 summarizes the functional security requirements needed to meet the security objectives listed in section 4. The mapping between objectives and requirements is given in section 6.3, which also explains the rationale behind the choices. Table 5.3 summarizes the assurance requirements that are consistent with the threat environment.